Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нилова Екатерина Викторовна
Должность: Директор
Дата подписания: 26.11.2026 20:49:29
Уникальный программный ключ:
01b497467f3626bb4aa4f462dec308bcc7b24a93

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

УТВЕРЖДАЮ
Заместитель директора по учебной работе
_____ /Л.А. Дьякова/
«26» июня 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02

разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования

по специальности 10.02.05 (код) Обеспечение информационной безопасности автоматизированных систем (Наименование специальности / профессии)

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
(Наименование дисциплины)

Кафедра разработчик Экономики и информационных дисциплин

Год набора 2023, 2024

2026 г.

Рабочая программа учебной практики по ПМ. 02
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
(наименование дисциплины согласно учебному плану)

Составлена *Кузнецовой Ириной Николаевной*
(Ф.И.О.)

Составлена _____
(Ф.И.О.)

Составлена _____
(Ф.И.О.)

Обсуждена и рекомендована к утверждению решением кафедры
экономики и информационных дисциплин
от 20.06.2026 г. протокол № 11
(дата протокола) *(номер протокола)*

Заведующий кафедрой _____ Мирошниченко Г.И.
(подпись) *(инициалы, фамилия)*

Согласовано с выпускающей кафедрой
экономики и информационных дисциплин

Заведующий кафедрой _____ Мирошниченко Г.И.
(подпись) *(инициалы, фамилия)*

Одобрена методическим советом

от 26.06.2026 протокол № 6
(дата протокола) *(номер протокола)*

_____ Л.А. Дьякова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02 ……..……..……. 6
2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02 ……..……... 12
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02 …... 15
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02 ……...…… 17

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПМ. 02

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Цель и место учебной практик в структуре образовательной программы

Цель учебной практики: освоение вида деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

Учебная практика включена в обязательную часть образовательной программы.

1.2. Планируемые результаты освоения учебной практики

Результаты освоения учебной практики соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения учебной практики обучающийся должен: освоить основной вид деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующие ему общие компетенции, профессиональные компетенции и личностные результаты:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ПК 2.1.	Осуществлять установку и настройку отдельных программных,

	программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2.3. В результате освоения учебной практики обучающийся должен:

Иметь практический опыт	В: – установке и настройке программных средств защиты информации; – тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; – учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – использовать типовые программные криптографические средства, в том числе электронную подпись; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; – основные понятия криптографии и типовых криптографических методов и средств защиты информации.

1.2.4. В результате освоения учебной практики в соответствии с профессиональным стандартом «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской

Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449), обучающийся должен выполнять трудовые действия:

Код	Трудовые действия
A/02.5	– текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями; – текущий, в том числе автоматизированный контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; – внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования; – восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД; – восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД;
A/03.5	– диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами; – обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД; – устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией; – направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; – ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

В результате освоения учебной практики в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 01 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)

Код	Трудовые действия
A/01.5	– ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах; – установка программно-аппаратных средств защиты информации; – настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам; – установка средств антивирусной защиты в соответствии с действующими

	требованиями; – инструктаж пользователей по порядку безопасной работы в операционных системах; – оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах; – восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации; – проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
A/02.5	– ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях; – установка программно-аппаратных средств защиты информации в компьютерных сетях; – установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации; – настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам; – устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации; – инструктаж пользователей по порядку безопасной работы в компьютерных сетях; – оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях;
A/03.5	– установка программного обеспечения; – настройка программного обеспечения с соблюдением требований по защите информации; – настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам; – инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением; – настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам; – проверка функционирования встроенных средств защиты информации программного обеспечения; – своевременное обнаружение признаков наличия вредоносного программного обеспечения.

В результате освоения учебной практики в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. №522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016г., регистрационный №43857), обучающийся должен выполнять трудовые действия:

Код	Трудовые действия
A/01.5	– контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации – контроль стабильности характеристик системы защиты информации автоматизированной системы;

A/02.5	– ведение документов учета, обработки, хранения и передачи информации, составляющей тайну – информирование персонала об угрозах безопасности информации – информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации – ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем – ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем – ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем;
A/03.5	– уничтожение информации, обрабатываемой автоматизированной системой – уничтожение машинных носителей информации, обрабатываемой автоматизированной системой – архивирование информации, обрабатываемой автоматизированной системой.

1.2.5. Перечень личностных результатов реализации программы воспитания

Код	**Личностные результаты реализации программы воспитания** *(дескрипторы)*
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
ЛР 16	Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством
ЛР 17	Открытый к текущим и перспективным изменениям в мире труда и профессий
ЛР 19	Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели)

	труда, либо иные схожие характеристики.
ЛР 20	Экономически активный, предприимчивый, готовый к самозанятости.

1.2. Цели и задачи учебной практики по ПМ. 02

Всего часов 108 часов

в том числе в форме практической подготовки 108 часов

Промежуточная аттестация дифференцированный зачет

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Тематический план и содержание учебной практики

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся		Объем часов
1	2		3
	Практические занятия		14
Тема 1.1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	1.	Применение аппаратно-программных модулей доверенной загрузки.	
	2.	Применение средств идентификации и аутентификации.	
	3.	Применение средств разграничения доступа.	
	4.	Применение средств аудита.	
	5.	Применение средств оперативного наблюдения.	
Тема 1.2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	Практические занятия		14
	1.	Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы операционной системы.	
	2.	Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	
	3.	Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных.	
Тема 1.3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	Практические занятия		8
	1.	Разработка системы показателей качества для методики оценки защищенности информации при эксплуатации информационной системы.	
	2.	Расчет по методике оценки эффективности защиты информации при эксплуатации программно-аппаратных средств обеспечения информационной безопасности в корпоративных сетях с разными требованиями по защищенности.	
Тема 1. 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	Практические занятия		6
	1.	Составление перечня коммерческих тайн и сведений, не подлежащих разглашению.	
	2.	Разработка способов хранения информации.	
	3.	Создание инструкций по защите секретных материалов, организация эффективной защиты компьютеров, локальных сетей.	
Тема 1.5. Использование	Практические занятия		20

программного обеспечения для обработки, хранения и передачи конфиденциальной информации	1.	Использование внешних компонентов средств контроля целостности автоматизированной системы и защиты информации.	
	2.	Использование компонентов защиты доступа к внутренним элементам технических средств.	
	3.	Настройка и использование DLP систем.	
	4.	Настройка и использование SIEM систем.	
	5.	Установка, настройка и использование ViPNet.	
Тема 1.6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	Практические занятия		
	1.	Анализ ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».	8
	2.	Проведение анализа исходной информации и объектов информатизации заказчика.	
	3.	Разработка программы и методики аттестационных испытаний.	
	4.	Проведение аттестационных испытаний объекта.	
Тема 1.7. Устранение замечаний по результатам проверки	1.	Анализ результаты проверки. Формирование сводных листов исправлений.	6
	2.	Анализ способов устранения замечаний. Устранение замечаний. Составление акта об устранении замечаний.	
	3.	Проведение повторных испытаний.	
Тема 1.8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов	1.	Анализ нормативной базы, регулирующей защиту программно-аппаратными средствами. Анализ внутренней среды организации.	4
	2.	Составление проекта внутреннего методического документа.	
Тема 1.9. Применение математических методов для оценки качества и выбора наилучшего программного средства	1.	Нечеткие множества: определение, свойства, операции над нечеткими множествами.	20
	2.	Нечеткая и лингвистическая логики.	
	3.	Обоснование показателя качества СЗИ.	
	4.	Методы построения функции принадлежности требований к СЗИ заданному уровню качества.	
	5.	Методы выбора рационального варианта средств защиты информации на основе экспертной информации.	
Тема 1.10. Использование	1.	Применение средств уничтожения остаточной информации.	8

типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	2.	Использование средств шифрования данных.	
	3.	Использование средств тестирования средств защиты информации.	
	4.	Использование средств сетевой защиты.	
	Всего:		108

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы учебной практики осуществляется в специализированном учебном кабинете.

Для проведения учебной практики специализированный учебный кабинет оснащается техническими средствами в количестве, необходимом для выполнения целей и задач практики: аудио-и видеозаписывающей и воспроизводящей аппаратурой, фотоаппаратурой, портативными и стационарными компьютерами с периферией (принтерами, сканерами), программным обеспечением, расходными материалами, канцелярскими принадлежностями, средствами связи, подключением к Интернет.

3.2. Информационное обеспечение обучения

3.2.1. Основные электронные издания

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2026. — 355 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01969-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2237199 (дата обращения: 11.11.2026)
2. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783
3. Внуков, А. А. Основы информационной безопасности: защита информации: учебник для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458
4. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом: учебник для вузов / Е. А. Войниканис; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589232
5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588246
6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. — Москва: ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2238628
7. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2026. — 424 с. — (Высшее

образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583156

8. Организационное и правовое обеспечение информационной безопасности: учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372

9. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва; Вологда: Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2169702

10. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584129

11. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. — Москва: ИНФРА-М, 2026. — 592 с. — (Высшее образование). - ISBN 978-5-16-022294-3. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2261229

12. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2026. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583858

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Образовательное учреждение обеспечивает организацию и проведение текущего контроля и промежуточной аттестации по учебной практике.

Текущий контроль проводится преподавателем в процессе обучения.

Обучение по учебной практике завершается итоговой аттестацией по учебной практике в форме дифференцированного зачета.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
Итоговая аттестация по учебной практике – дифференцированный зачет		

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	демонстрация ответственности за принятые решения; обоснованность самоанализа и коррекция результатов собственной работы	
Эффективно взаимодействовать и работать в коллективе и команде	взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	грамотность устной и письменной речи; ясность формулирования и изложения мыслей	
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе	соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	

традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения		
Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	
Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	